

(12) 发明专利申请

(10) 申请公布号 CN 102521626 A

(43) 申请公布日 2012. 06. 27

(21) 申请号 201110391460. 8

(22) 申请日 2011. 11. 30

(71) 申请人 北京握奇数据系统有限公司

地址 100015 北京市朝阳区东直门外西八间
房万红西街 2 号燕东商务花园

(72) 发明人 雷霆 温丽明

(74) 专利代理机构 北京润泽恒知识产权代理有
限公司 11319

代理人 苏培华

(51) Int. Cl.

G06K 17/00 (2006. 01)

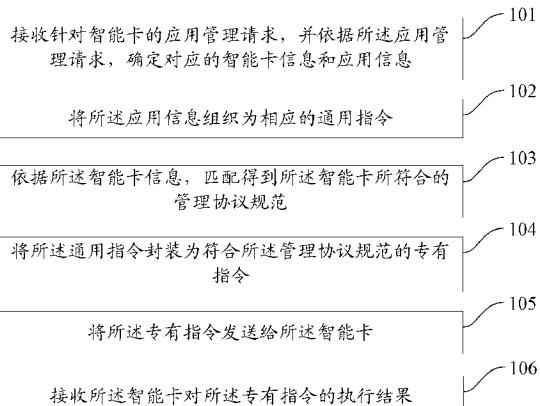
权利要求书 2 页 说明书 12 页 附图 4 页

(54) 发明名称

一种智能卡的多应用管理方法和系统

(57) 摘要

本申请提供了一种智能卡的多应用管理方法和系统,其中的方法具体包括:接收针对智能卡的应用管理请求,并依据所述应用管理请求,确定对应的智能卡信息和应用信息;将所述应用信息组织为相应的通用指令;依据所述智能卡信息,匹配得到所述智能卡所符合的管理协议规范;将所述通用指令封装为符合所述管理协议规范的专有指令;将所述专有指令发送给所述智能卡;接收所述智能卡对所述专有指令的执行结果。本申请能够灵活地适用于各种管理协议规范的智能卡的多应用管理。



1. 一种智能卡的多应用管理方法,其特征在于,包括:

接收针对智能卡的应用管理请求,并依据所述应用管理请求,确定对应的智能卡信息和应用信息;

将所述应用信息组织为相应的通用指令;

依据所述智能卡信息,匹配得到所述智能卡所符合的管理协议规范;

将所述通用指令封装为符合所述管理协议规范的专有指令;

将所述专有指令发送给所述智能卡;

接收所述智能卡对所述专有指令的执行结果。

2. 根据权利要求 1 所述的方法,其特征在于,所述将所述应用信息组织为相应的通用指令的步骤,包括:

依据预置的通用指令的数据格式,通过填充字段方式将所述应用信息组织为相应的通用指令。

3. 根据权利要求 1 所述的方法,其特征在于,所述将所述通用指令封装为符合所述管理协议规范的专有指令的步骤,包括:

依据所述通用指令,匹配得到相应的转换规则;

利用所述转换规则对所述通用指令进行转换,得到相应的转换结果;

依据所述转换结果,通过填充字段方式得到符合所述管理协议规范的专有指令。

4. 根据权利要求 3 所述的方法,其特征在于,所述依据所述通用指令,匹配得到相应的转换规则的步骤为,依据所述通用指令中第二字段的值,匹配得到第一字段的转换规则。

5. 根据权利要求 3 所述的方法,其特征在于,所述利用所述转换规则对所述通用指令进行转换的步骤为,根据第三字段的正则匹配关系对第四字段进行匹配,得到相应的转换结果。

6. 根据权利要求 1 所述的方法,其特征在于,所述将所述应用信息组织为相应的通用指令的步骤,包括:

依据通信通道所符合的管理协议规范中规定的数据字段长度,对所述应用信息进行分组;

分别将各组的应用信息组织为相应的通用指令。

7. 根据权利要求 1 所述的方法,其特征在于,还包括:

在接收某一智能卡对所述专有指令的执行结果时,依据该智能卡所符合的管理协议规范将所述执行结果解析为通用结果;

将所述通用结果解析为业务数据,并依据所述业务数据进行相应的业务处理。

8. 根据权利要求 1 所述的方法,其特征在于,所述智能卡信息包括智能卡的序列号,或者类别,或者支持的管理协议规范类别,或者版本。

9. 根据权利要求 1 至 8 中任一项所述的方法,其特征在于,所述应用管理请求来自如下一种或多种行业领域中的管理系统:金融、通信、交通,所述管理系统包括卡管系统和 / 或用户管理系统。

10. 一种智能卡的多应用管理系统,其特征在于,包括:

业务处理模块,用于接收针对智能卡的应用管理请求,并依据所述应用管理请求,确定对应的智能卡信息和应用信息;

通用指令组织模块,用于将所述应用信息组织为相应的通用指令;
匹配模块,用于依据所述智能卡信息,匹配得到所述智能卡所符合的管理协议规范;
专有指令封装模块,用于将所述通用指令封装为符合所述管理协议规范的专有指令;
发送模块,用于将所述专有指令发送给所述智能卡;及
接收模块,用于接收所述智能卡对所述专有指令的执行结果。

11. 根据权利要求 10 所述的系统,其特征在于,所述通用指令组织模块,包括:

填充组织子模块,用于依据预置的通用指令的数据格式,通过填充字段方式将所述应用信息组织为相应的通用指令。

12. 根据权利要求 10 所述的系统,其特征在于,所述专有指令封装模块,包括:

规则匹配子模块,用于依据所述通用指令,匹配得到相应的转换规则;

转换子模块,用于利用所述转换规则对所述通用指令进行转换,得到相应的转换结果;

填充封装子模块,用于依据所述转换结果,通过填充字段方式得到符合所述管理协议规范的专有指令。

13. 根据权利要求 12 所述的系统,其特征在于,所述规则匹配子模块,具体用于依据所述通用指令中第一字段的值,匹配得到第二字段的转换规则。

14. 根据权利要求 12 所述的系统,其特征在于,所述转换子模块,具体用于根据第三字段的正则匹配关系对第四字段进行匹配,得到相应的转换结果。

15. 根据权利要求 10 所述的系统,其特征在于,所述通用指令组织模块,包括:

分组子模块,用于依据通信通道所符合的管理协议规范中规定的数据字段长度,对所述应用信息进行分组;

组织子模块,用于分别将各组的应用信息组织为相应的通用指令。

16. 根据权利要求 10 所述的系统,其特征在于,还包括:

第一解析模块,用于在接收某一智能卡对所述专有指令的执行结果时,依据该智能卡所符合的管理协议规范将所述执行结果解析为通用结果;

第二解析模块,用于将所述通用结果解析为业务数据;

业务处理模块,用于依据所述业务数据进行相应的业务处理。

17. 根据权利要求 10 所述的系统,其特征在于,所述智能卡信息包括智能卡的序列号,或者类别,或者支持的管理协议规范类别,或者版本。

18. 根据权利要求 10 至 17 中任一项所述的系统,其特征在于,所述应用管理请求来自如下一种或多种行业领域中的管理系统:金融、通信、交通,所述管理系统包括卡管系统和 / 或用户管理系统。

一种智能卡的多应用管理方法和系统

技术领域

[0001] 本申请涉及智能卡应用管理技术领域,特别是涉及一种智能卡的多应用管理方法和系统。

背景技术

[0002] 目前,随着智能卡应用的不断增加和日益普及,用户需要拥有和携带的智能卡也越来越多,例如网上银行支付卡、电子交易卡、电子交通卡等。虽然不断增多的智能卡数量和种类提高了用户使用智能卡的成本,但也给智能卡的管理带了不便。

[0003] 为了克服上述管理不便的问题,现有一种智能卡的多应用管理方法将应用信息预置在智能卡内,即在生产智能卡过程中,就已经将应用及个人化信息预置在智能卡内,这种方式的缺点是应用及个人化信息固化在智能卡上,缺乏灵活性。

[0004] 针对上述缺乏灵活性的问题,现有另一种智能卡的多应用管理方法在智能卡开通使用之前,利用 OTA(空中下载, Over The Air) 技术或者 POS(销售终端, Point Of Sale) 等设备进行应用下载及个人化。

[0005] 然而,第二种方法只是针对符合某一种规范的智能卡进行特定的应用管理;当前全球存在多种智能卡规范,如 ISO-7816 系列、GP(Global Platform) 系列、MULTOS(多应用操作系统, Multi-application Operation System,) 系列等,如果第二种方法只能针对符合 GP 规范的智能卡做应用管理,那么对于符合 MULTOS 系列的智能卡就不适用了。

[0006] 总之,需要本领域技术人员迫切解决的一个技术问题就是:如何能够提供一种通用的、适用于各种管理协议规范的智能卡的多应用管理方法。

发明内容

[0007] 本申请所要解决的技术问题是提供一种智能卡的多应用管理方法和系统,能够灵活地适用于各种管理协议规范的智能卡的多应用管理。

[0008] 为了解决上述问题,本申请公开了一种智能卡的多应用管理方法,包括:

[0009] 接收针对智能卡的应用管理请求,并依据所述应用管理请求,确定对应的智能卡信息和应用信息;

[0010] 将所述应用信息组织为相应的通用指令;

[0011] 依据所述智能卡信息,匹配得到所述智能卡所符合的管理协议规范;

[0012] 将所述通用指令封装为符合所述管理协议规范的专有指令;

[0013] 将所述专有指令发送给所述智能卡;

[0014] 接收所述智能卡对所述专有指令的执行结果。

[0015] 优选的,所述将所述应用信息组织为相应的通用指令的步骤,包括:

[0016] 依据预置的通用指令的数据格式,通过填充字段方式将所述应用信息组织为相应的通用指令。

[0017] 优选的,所述将所述通用指令封装为符合所述管理协议规范的专有指令的步骤,

包括：

- [0018] 依据所述通用指令，匹配得到相应的转换规则；
- [0019] 利用所述转换规则对所述通用指令进行转换，得到相应的转换结果；
- [0020] 依据所述转换结果，通过填充字段方式得到符合所述管理协议规范的专有指令。
- [0021] 优选的，所述依据所述通用指令，匹配得到相应的转换规则的步骤为，依据所述通用指令中第二字段的值，匹配得到第一字段的转换规则。
- [0022] 优选的，所述利用所述转换规则对所述通用指令进行转换的步骤为，根据第三字段的正则匹配关系对第四字段进行匹配，得到相应的转换结果。
- [0023] 优选的，所述将所述应用信息组织为相应的通用指令的步骤，包括：
- [0024] 依据通信通道所符合的管理协议规范中规定的数据字段长度，对所述应用信息进行分组；
- [0025] 分别将各组的应用信息组织为相应的通用指令。
- [0026] 优选的，所述方法还包括：
- [0027] 在接收某一智能卡对所述专有指令的执行结果时，依据该智能卡所符合的管理协议规范将所述执行结果解析为通用结果；
- [0028] 将所述通用结果解析为业务数据，并依据所述业务数据进行相应的业务处理。
- [0029] 优选的，所述智能卡信息包括智能卡的序列号，或者类别，或者支持的管理协议规范类别，或者版本。
- [0030] 优选的，所述应用管理请求来自如下一种或多种行业领域中的管理系统：金融、通信、交通，所述管理系统包括卡管系统和 / 或用户管理系统。
- [0031] 另一方面，本申请还公开了一种智能卡的多应用管理系统，包括：
- [0032] 业务处理模块，用于接收针对智能卡的应用管理请求，并依据所述应用管理请求，确定对应的智能卡信息和应用信息；
- [0033] 通用指令组织模块，用于将所述应用信息组织为相应的通用指令；
- [0034] 匹配模块，用于依据所述智能卡信息，匹配得到所述智能卡所符合的管理协议规范；
- [0035] 专有指令封装模块，用于将所述通用指令封装为符合所述管理协议规范的专有指令；
- [0036] 发送模块，用于将所述专有指令发送给所述智能卡；及
- [0037] 接收模块，用于接收所述智能卡对所述专有指令的执行结果。
- [0038] 优选的，所述通用指令组织模块，包括：
- [0039] 填充组织子模块，用于依据预置的通用指令的数据格式，通过填充字段方式将所述应用信息组织为相应的通用指令。
- [0040] 优选的，所述专有指令封装模块，包括：
- [0041] 规则匹配子模块，用于依据所述通用指令，匹配得到相应的转换规则；
- [0042] 转换子模块，用于利用所述转换规则对所述通用指令进行转换，得到相应的转换结果；
- [0043] 填充封装子模块，用于依据所述转换结果，通过填充字段方式得到符合所述管理协议规范的专有指令。

[0044] 优选的，所述规则匹配子模块，具体用于依据所述通用指令中第一字段的值，匹配得到第二字段的转换规则。

[0045] 优选的，所述转换子模块，具体用于根据第三字段的正则匹配关系对第四字段进行匹配，得到相应的转换结果。

[0046] 优选的，所述通用指令组织模块，包括：

[0047] 分组子模块，用于依据通信通道所符合的管理协议规范中规定的数据字段长度，对所述应用信息进行分组；

[0048] 组织子模块，用于分别将各组的应用信息组织为相应的通用指令。

[0049] 优选的，所述系统还包括：

[0050] 第一解析模块，用于在接收某一智能卡对所述专有指令的执行结果时，依据该智能卡所符合的管理协议规范将所述执行结果解析为通用结果；

[0051] 第二解析模块，用于将所述通用结果解析为业务数据；

[0052] 业务处理模块，用于依据所述业务数据进行相应的业务处理。

[0053] 优选的，所述智能卡信息包括智能卡的序列号，或者类别，或者支持的管理协议规范类别，或者版本。

[0054] 优选的，所述应用管理请求来自如下一种或多种行业领域中的管理系统：金融、通信、交通，所述管理系统包括卡管系统和 / 或用户管理系统。

[0055] 与现有技术相比，本申请包括以下优点：

[0056] 首先，相对于现有技术直接对业务数据进行封装，本申请首先将应用信息标识的业务数据组织为通用数据格式，然后，根据当前智能卡所符合的管理协议规范，将所述通用数据格式转换为当前智能卡能有效执行的专用数据格式；因此，能够满足对符合不同管理协议规范的智能卡，统一进行应用管理的需求，具有好的通用性；

[0057] 其次，相对于现有技术将应用及个人化信息固化在智能卡上，本申请可以在智能卡开通使用之前甚至开通使用过程中，进行智能卡的应用管理，并且，其可适用于电信、金融、通信、交通等不同领域，适用于 native 卡、java 卡、MULTOS 卡等不同智能卡种类，适用于 SIM、microSD、金融 PBOC 卡等不同卡片物理形态的多应用管理；因此，本申请具有好的灵活性；

[0058] 再者，由于本申请能够将通用指令封装为符合所述管理协议规范的专有指令，所以封装或者仅需制定通用指令与专有指令之间的对应关系，或者，制定通用指令与专有指令之间的转换规则；这样，欲增加管理协议规范时，只需依据欲增加管理协议规范，制定相应的通用指令与专有指令之间的对应关系或转换规则即可，因此，本申请具有好的扩展性。

附图说明

[0059] 图 1 是本申请一种智能卡的多应用管理方法实施例的流程图；

[0060] 图 2 是本申请一种多应用管理系统的结构示意图；

[0061] 图 3 是图 2 所示多应用管理系统的工作流程；

[0062] 图 4 是本申请一种智能卡的多应用管理系统实施例的结构图。

具体实施方式

[0063] 为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

[0064] 现有技术只能针对符合某一种规范的智能卡进行特定的应用管理，所以，在接收针对智能卡的应用管理请求时，能够依据所述应用管理请求，确定对应的业务数据，并直接将所述业务数据封装为符合某一种管理协议规范的智能卡能有效执行的 APDU(应用协议数据单元，Application Protocol Data Unit) 指令；也即，现有技术只能将业务数据封装为符合某一种管理协议规范的智能卡能有效执行的指令，故不具备通用性。

[0065] 本申请实施例的核心构思之一在于，不是直接对业务数据进行封装，而是首先将业务数据组织为通用数据格式，然后，根据当前智能卡所符合的管理协议规范，将所述通用数据格式转换为当前智能卡能有效执行的专用数据格式；因此，能够满足对符合不同管理协议规范的智能卡，统一进行应用管理的需求。

[0066] 参照图 1，示出了本申请一种智能卡的多应用管理方法实施例的流程图，具体可以包括：

[0067] 步骤 101、接收针对智能卡的应用管理请求，并依据所述应用管理请求，确定对应的智能卡信息和应用信息；

[0068] 在实际中，可由用户、卡管系统、用户管理系统等发起应用管理请求；例如，用户可通过 web(万维网) 页面或者手机客户端方式发起应用管理请求。所述应用管理主要可以包括：应用信息查询、应用下载、应用个人化、应用生命周期管理等。

[0069] 在实际应用中，所述智能卡信息一般存在于卡片描述文件中，所以通常获取的就是卡片描述文件；其中，所述卡片描述文件通过卡片管理接口存放智能卡的关键信息，通常一张卡片对应一个卡片描述文件。

[0070] 所述应用信息可以看作用于处理应用管理请求的业务数据。为了准确的获得针对智能卡的应用管理请求对应的应用信息，在本申请的一种应用示例中，所述应用管理请求中可以具体包括：应用标识以及应用指令；

[0071] 其中，应用标识，可以用于确定所述应用管理请求对应的应用管理类型，属于应用信息查询、应用下载、应用个人化、应用生命周期管理等中的哪一者。在实际中，可以采用 ISO(国际标准化组织，International Organization for Standardization) 全球统一分配原则，根据 ISO 标识规定的应用标识与应用管理类型的对应关系，确定该应用标识对应应该管理类型。或者，也可以根据实际情况建立应用标识和应用下载类型的对应关系，如应用信息查询用应用标识 01 代码表示，应用下载用应用标识 02 代码表示，并将所述对应关系保存在数据库中，在获取时通过查找数据库确定应用下载类型即可。

[0072] 应用指令，可以用于确定所述应用下载请求对应的操作类型。以电信领域的智能卡为例，该应用指令需要符合特定规范（如中国移动规定的 GSM11.14 规范），这样就可以对该应用指令进行解析，并确定对应的操作类型。所述操作类型可以包括对电信智能卡所承载的应用进行的各种处理，如如下中的任意一个：激活应用、暂停应用、取消暂停应用、终止应用等。

[0073] 上面对确定与所述应用下载请求对应的应用信息做了详细说明，可以理解，上面仅是示例，实际上，本申请对应用信息的确定方式不加以限制。

[0074] 步骤 102、将所述应用信息组织为相应的通用指令；

[0075] 本步骤在技术方案中起承上启下的衔接作用,其在将上层的应用信息组织为相应的通用指令后,输出的是统一的通用指令接口,下层只需要处理通用指令数据就可以了。例如,在接收到所述应用信息表示的业务数据时,为了能够将所述应用信息下发给符合不同管理协议规范的智能卡,本步骤首先将这些业务数据封装成通用的数据格式,由下层根据当前智能卡所符合的管理协议规范,将所述通用数据格式转换为当前智能卡能有效执行的专用数据格式。

[0076] 在本申请实施例中,所述通用指令主要表示为了实现通用性,为应用信息和智能卡能用有效执行的指令提供的中间指令状态。在具体实现中,可以依据各种管理协议规范,预置通用指令的数据格式。参照表1,示出了本申请一种通用指令的数据格式示例,其中,通用指令可以预置一套 INS 字段,具体标识指令类型(如,定义 05 表示存储数据指令),等。

[0077] 表 1 通用指令的数据格式

[0078]

字段名	字段值	字段说明
CLA	00	识别字节
INS	00-FF	指令字节,存储指令(05)
P1	00-FF	加密标识
P2	00-FF	加密算法
P3	00-FF	数据块总数
P4	00-FF	数据块索引
Lc 字段	XX	后续数据字段的长度

[0079]

数据字段	XXXX...	数据
Le 字段	空	

[0080] 这样,在本申请的一种优选实施例中,所述将所述应用信息组织为相应的通用指令的步骤,可以包括:

[0081] 依据预置的通用指令的数据格式,通过填充字段方式将所述应用信息组织为相应的通用指令。

[0082] 所述填充字段方式的原理主要是依据所述应用信息对预置的通用指令的数据格式中的各字段进行赋值,并组织给通用指令的过程。以表 1 所示的通用指令的数据格式为例,CLA 字段的值固定为 00,对于不同的应用信息,INS 字段的值通常是不同的,例如,应用下载类型对应的 INS 字段的值为 00,而应用个人化类型对应的 INS 的值为 01;另外,P1,P2,P3,P4 的值也需要根据具体的应用信息来确定和填充。本申请对具体的通用指令的数据格式、通用指令的数据格式各字段值的确定方式和填充方式不加以限制。

[0083] 在实际应用中,有些应用信息是必须加密的,如应用服务器(银行卡应用服务器)跟智能卡之间的通信密钥,用户智能卡的校验信息等,这些应用信息一旦泄露,卡片就可以被复制,所以一定要加密。

[0084] 因此,在本申请的一种优选实施例中,本步骤还可以在组织通用指令的过程中,依据应用信息,对其中的关键业务数据进行加解密处理。

[0085] 步骤 103、依据所述智能卡信息,匹配得到所述智能卡所符合的管理协议规范;

[0086] 在实际应用中,获取得到的卡片描述文件中通常包括智能卡的序列号,或者类别,或者支持的管理协议类别,或者版本等智能卡信息。通过这些智能卡信息,可以匹配得到卡片符合哪种管理协议规范。其中,匹配规则可以为,规定某个类型或某个范围的卡片序列号适用一种具体的管理协议规范。在具体实现中,可以将一种具体管理协议规范的卡片序列号存储在数据库中,通过查找数据库的方式来完成所述匹配。

[0087] 对于类别,或者支持的操作系统类别,或者版本等智能卡信息的匹配,由于与卡片序列号的匹配相似,故在此不作赘述,相互参照即可。

[0088] 步骤 104、将所述通用指令封装为符合所述管理协议规范的专有指令;

[0089] 本步骤根据当前智能卡所符合的管理协议规范,将所述通用数据格式转换为当前智能卡能有效执行的专用数据格式。

[0090] 当前全球存在多种智能卡的管理协议规范,如 ISO-7816 系列、GP 系列、MULTOS 系列,这三种管理协议规范在报文结构上是相同的,由 CLA、INS、P1、P2、Lc 字段、数据字段、Le 字段组成。但是在每个字段具体定义上有区别,以存储指令为例,ISO/IEC7816 结构如表 2 所示,GP 结构如表 3 所示,MULTOS 结构如表 4 所示。

[0091] 表 2ISO/IEC7816 存储指令结构

[0092]

字段名	字段值	字段说明
CLA	00-FF	识别字节
INS	DA	指令字节, put_data
P1	00 - FF	参数字节, 共同控制数据字段
P2	00 - FF	
Lc字段	XX	后续数据字段的长度
数据字段	XXXX...	数据
Le字段	空	

[0093] 表 3GP 存储指令结构

[0094]

字段名	字段值	字段说明
CLA	80-8F/C0-CF/E0-EF	识别字节

[0095]

INS	E2	指令字节, store data
P1	00-FF	控制参数
P2	00-FF	数据块序号
Lc 字段	XX	后续数据字段的长度
数据字段	XXXX...	数据
Le 字段	空	

[0096] 表 4MULTOS 存储指令结构

[0097]

字段名	字段值	字段说明
CLA	BE	识别字节
INS	26	指令字节, put_data
P1	00 - FF	偏移量控制参数
P2	00 - FF	
Lc字段	XX	后续数据字段的长度
数据字段	XXXX...	数据
Le字段	空	

[0098] 上面对 ISO-7816 系列、GP 系列、MULTOS 系列的存储指令结构进行了举例说明,需要说明的是,上述说明仅是作为示例,但并不能作为本申请的限制;另外,本申请也不限于上述三种管理协议规范,实际上,任意的管理协议规范都是可行的。

[0099] 对于某些字段(如 INS)而言,可以制定通用指令与专有指令的对应关系,然后利

用对应关系进行简单替换即可。

[0100] 对于另外一些字段（如 CLA、P1、P2）而言，则需要制定一定的转换规则，且这个转换规则不是简单替换，而是一些相对复杂的规则，如替换、拼接、位移、异或等规则中的一种或多种。

[0101] 在本申请的一种优选实施例中，所述将所述通用指令封装为符合所述管理协议规范的专有指令的步骤，可以进一步包括：

[0102] 子步骤 A1、依据所述通用指令，匹配得到相应的转换规则；

[0103] 以表 3 所示 GP 存储指令结构中 CLA 字段的转换为例，在有些情况下，可以定义一些简单的转换规则将“00”转换为“00”或者“80”或者“84”中的一者，此时无需进行转换规则的匹配。

[0104] 在本申请的一种优选实施例中，所述依据所述第二字段的值，匹配得到第一字段的转换规则。

[0105] 前面提到，通用指令可以预置一套 INS 字段，用于具体标识指令类型的，那么，可以对于不同的 INS 制定不同的转换规则。

[0106] 例如，可以定义 INS 字段的匹配规则 M1，M2（以正则表达式的方式定义），定义两个转换规则 T1，T2；如果 INS 字段的值满足匹配规则 M1，则可直接利用转换规则 T1 将 CLA 替换为“00”；如果 INS 字段的值满足匹配规则 M2，则可以利用转换规则 T2 及 P2 字段的值，对 CLA 进行转换。

[0107] 对于 P1、P2，由于转换规则的匹配过程与 CLA 类似，故在此不作赘述，相互参照即可。

[0108] 子步骤 A2、利用所述转换规则对所述通用指令进行转换，得到相应的转换结果；

[0109] 通常情况下，一种字段的转换规则可以与其它字段无关，如转换规则 T1 将 CLA 替换为“00”。

[0110] 在某些特殊情况下，一种字段的转换规则还需用到其它字段。在本申请的另一种实施例中，所述利用所述转换规则对所述通用指令进行转换的步骤可以为，根据第三字段的正则匹配关系对第四字段进行匹配，得到相应的转换结果。

[0111] 例如，利用转换规则 T2 对 CLA 进行转换时，所述 T2 转换规则可以为根据加密算法标识 P2 的正则匹配关系，如果是 DES 加密算法 01，即转换为“80”，如果是 DES-CBC 算法 02，即转化为“84”。

[0112] 在实际中，可以将上述两种实施例结合起来使用，例如对于表 2- 表 4 所述的三种管理协议规范的存储指令结构，对表格中各字段进行标号，得到字段 1- 字段 6（CLA- 数据字段），则所述结合使用可以为，根据字段 2 的正则匹配关系，匹配得到字段 3 及字段 4 的转换规则，根据字段 3- 字段 6 的值，得到字段 3 及字段 4 的转换结果。

[0113] 子步骤 A3、依据所述转换结果，通过填充字段方式得到符合所述管理协议规范的专有指令。

[0114] 所述填充字段方式的原理主要是依据所述转换结果对所述管理协议规范中的各字段进行赋值，并封装为专有指令（如 APDU 指令）的过程。

[0115] 以表 3 所示 GP 存储指令结构为例，假设下发的应用数据是第一条且是需要加密的，则可以封装得到如下专有指令：84 E2 60 01 06 209039393039，其中，空格是不存在

的,是为了说明而分开的,“84”是标识字节,“E2”是固定值,“60”表示加密,“01”表示数据块序号,“06”表示数据字段的字节长度是6字节,“20A0E9393039”表示后续字节。

[0116] 总之,本步骤能够根据当前智能卡所符合的管理协议规范,将所述通用数据格式转换为当前智能卡能有效执行的专用数据格式。

[0117] 步骤105、将所述专有指令发送给所述智能卡;

[0118] 步骤106、接收所述智能卡对所述专有指令的执行结果。

[0119] 在实际应用中,本申请与智能卡之间可以通过Internet(因特网)、SMS(短消息服务short message services)、GSM(全球移动通讯系统,global system for mobile communications)或者GPRS(通用分组无线服务技术,General Packet Radio Service)等通讯方式中的一者进行通讯,本申请对针对智能卡的具体通讯方式不加以限制。

[0120] 总之,本申请具有如下优点:

[0121] 1、相对于现有技术直接对业务数据进行封装,本申请首先将应用信息标识的业务数据组织为通用数据格式,然后,根据当前智能卡所符合的管理协议规范,将所述通用数据格式转换为当前智能卡能有效执行的专用数据格式;因此,能够满足对符合不同管理协议规范的智能卡,统一进行应用管理的需求,具有好的通用性;

[0122] 2、相对于现有技术将应用及个人化信息固化在智能卡上,本申请可以在智能卡开通使用之前甚至开通使用过程中,进行智能卡的应用管理,并且,其可适用于电信、金融、通信、交通等不同领域,适用于native卡、java卡、MULTOS卡等不同智能卡种类,适用于SIM(用户身份识别模块,Subscriber Identity Module)、microSD(快闪存储器卡)、金融PBOC(中国人民银行,The People's Bank of China)卡等不同卡片物理形态的多应用管理;因此,本申请具有好的灵活性;

[0123] 3、由于本申请能够将通用指令封装为符合所述管理协议规范的专有指令,所以封装或者仅需制定通用指令与专有指令之间的对应关系,或者,制定通用指令与专有指令之间的转换规则;这样,欲增加管理协议规范时,只需依据欲增加管理协议规范,制定相应的通用指令与专有指令之间的对应关系或转换规则即可,因此,本申请具有好的扩展性。

[0124] 根据表2、表3、表4所示管理协议规范的存储指令结构示例,可以看出,这些管理协议规范的存储指令结构中的Lc字段对后续数据字段的长度作出了规定,也即,后续数据字段的长度是有限制的。

[0125] 因此,为了防止欲下发专有指令的后续数据字段的长度超出规定,在本申请的一种优选实施例中,所述将所述应用信息组织为相应的通用指令的步骤,可以包括:

[0126] 依据通信通道所符合的管理协议规范中规定的数据字段长度,对所述应用信息进行分组;

[0127] 分别将各组的应用信息组织为相应的通用指令。

[0128] 例如,所述应用信息所标识业务数据的长度为1k,1k的长度容易超出后续数据字段的长度的规定,则在实际中,可以将1k的业务数据分为2组,分别得到2个通用指令和相应的2个专有指令,然后下发给智能卡。

[0129] 需要说明的是,这里的分组数目还可以是2组以上,其可以根据经验值或者预置来确定。本申请的目的是为了防止欲下发专有指令的后续数据字段的长度超出规定,而不会对具体的分组方式和分组数目加以限制。

- [0130] 在本申请的另一种优选实施例中,所述方法还可以包括:
- [0131] 在接收某一智能卡对所述专有指令的执行结果时,依据该智能卡所符合的管理协议规范将所述执行结果解析为通用结果;
- [0132] 将所述通用结果解析为业务数据,并依据所述业务数据进行相应的业务处理。
- [0133] 在将专有指令下发给智能卡后,智能卡执行指令,但是智能卡可能执行成功,也可能执行失败。所以需要对所述专有指令的执行结果进行处理,以应用下载为例,只有智能卡执行成功后,才能绑定用户及应用下载的对应关系,某些情况下还需要把处理结果再上报给卡管系统。
- [0134] 在实际应用中,智能卡上行返回的所述专有指令的执行结果通常包括智能卡执行状态 + 执行内容,本申请的处理流程通常包括:
- [0135] 首先,对这个执行结果进行解析得到通用结果,解析过程可以为:如果专有指令执行成功,则将相应的执行结果转化为“9000+ 执行内容”,如果专有指令执行失败,则将相应的执行结果转化为“智能卡执行状态(可预置,非 9000+ 执行内容)”;
- [0136] 然后,会继续对通用结果进行解析,例如,可以将“9000+ 执行内容”转化为“状态表示 + 执行内容”,所述状态表示的一个例子可以是,“00”表示成功,“01”表示密钥不正确,“02”表示解析失败等;
- [0137] 最后,根据状态表示再做相关处理。
- [0138] 对于依据该智能卡所符合的管理协议规范将所述执行结果解析为通用结果的步骤,由于其是步骤 104 的逆过程;对于将所述通用结果解析为业务数据的步骤,由于其是步骤 102 的逆过程,故在此不作赘述,相互参照即可。
- [0139] 在实际中,所述业务处理还可以包括记录相关信息、中断后续的处理命令等;在某些情况下,还需要将处理结果再上传给给卡管系统;必要时,如应用个人化,还需要将执行结果以短信的方式通知用户。
- [0140] 在实际应用中,可以将本申请的方法集成在多应用管理系统中,参照图 2,示出了本申请一种多应用管理系统的结构示意图,具体可以包括:
- [0141] 业务处理层 201,其主要用于对应用管理请求进行处理,所述处理主要可以包括:记录智能卡信息;记录智能卡及应用的绑定信息;记录用户的操作日志信息;从卡管系统获取必要的信息(如:应用数据,应用个性化数据),校验并组织相关数据;将用户对智能卡的操作(如应用禁用),组织成报文,上传给卡管系统等;辅助地,其还用于与卡管(用户管理)系统进行通信;
- [0142] 通用指令层 202,作为中间层,其主要用于上下层之间的衔接;针对上下层来说,经过通用指令层转换后,它输出的是统一通用的指令接口,上下层只需要处理通用的指令数据就可以了,例如,通用指令层接收到业务处理层的处理数据,需要下发给不同种类的智能卡,首先是将这些处理数据封装成通用的数据格式,转换层接收到通用数据格式后,再根据智能卡协议种类,再进行转换;另外,其还可以将智能卡返回的通用结果集解析为业务数据传递给业务处理层 201;某些情况下,其还可以对关键数据进行加解密处理;
- [0143] 指令转换及自适应层 203,其可以根据卡片种类的不同,应用领域的不同,将通用指令集封装为不同管理协议规范(如 ISO/IEC7816、GP、MULTOS 等)的专用指令集,提供给智能卡进行有效执行;以及,可以将智能卡返回的专用结果集解析为通用结果集,传递给通

用指令层 202 ;及

[0144] 通讯接口层 204,用于调用 GSM、GPRS、Internet 等通道,将专有指令发送给智能卡 ;以及,将智能卡处理结果信息返回给指令转换及自适应层 203。

[0145] 为使本领域技术人员更好地理解本申请,下面以应用下载为例,说明图 2 所示多应用管理系统(等同于多应用管理平台)的工作流程,参照图 3,具体可以包括:

[0146] 步骤 1、用户申请应用下载;

[0147] 步骤 2、多应用管理平台的业务处理层验证用户的合法性,并获取该用户的智能卡信息,获取用户所选择的应用信息及应用文件;

[0148] 步骤 3、多应用管理平台的通用指令层将应用信息及应用文件组织为分组的通用指令集;

[0149] 步骤 4、多应用管理平台的指令转换及自适应层判断智能卡信息,利用转化规则,将通用指令集转换为智能卡能有效执行的专有 APDU 指令;

[0150] 步骤 5、多应用管理平台的通讯接口层将专有 APDU 指令发送给智能卡;

[0151] 步骤 6、智能卡执行后,将相应的执行结果返回给多应用管理平台的通讯接口层;

[0152] 步骤 7、通讯接口层将所述执行结果转给指令转换及自适应层,由指令转换及自适应层解析结果报文,并经过通用指令层转换为业务数据,传送给业务处理层;

[0153] 步骤 8、多应用管理平台的业务处理层处理智能卡返回结果,并向卡管系统上报应用下载结果。

[0154] 参照图 4,示出了本申请一种智能卡的多应用管理系统实施例的结构图,具体可以包括:

[0155] 业务处理模块 401,用于接收针对智能卡的应用管理请求,并依据所述应用管理请求,确定对应的智能卡信息和应用信息;

[0156] 通用指令组织模块 402,用于将所述应用信息组织为相应的通用指令;

[0157] 匹配模块 403,用于依据所述智能卡信息,匹配得到所述智能卡所符合的管理协议规范;

[0158] 专有指令封装模块 404,用于将所述通用指令封装为符合所述管理协议规范的专有指令;

[0159] 发送模块 405,用于将所述专有指令发送给所述智能卡;及

[0160] 接收模块 406,用于接收所述智能卡对所述专有指令的执行结果。

[0161] 在本申请实施例中,优选的是,所述智能卡信息具体可以包括智能卡的序列号,或者类别,或者支持的管理协议规范类别,或者版本。

[0162] 在本申请的一种优选实施例中,所述通用指令组织模块 402 可以进一步包括:

[0163] 填充组织子模块,用于依据预置的通用指令的数据格式,通过填充字段方式将所述应用信息组织为相应的通用指令。

[0164] 在本申请的另一种优选实施例中,所述专有指令封装模块 404 可以进一步包括:

[0165] 规则匹配子模块,用于依据所述通用指令,匹配得到相应的转换规则;

[0166] 转换子模块,用于利用所述转换规则对所述通用指令进行转换,得到相应的转换结果;及

[0167] 填充封装子模块,用于依据所述转换结果,通过填充字段方式得到符合所述管理

协议规范的专有指令。

[0168] 在本申请实施例中，优选的是，所述规则匹配子模块，具体用于依据所述通用指令中第一字段的值，匹配得到第二字段的转换规则。

[0169] 在本申请实施例中，优选的是，所述转换子模块，具体用于根据第三字段的正则匹配关系对第四字段进行匹配，得到相应的转换结果。

[0170] 在本申请的再一种优选实施例中，所述通用指令组织模块402，可以进一步包括：

[0171] 分组子模块，用于依据通信通道所符合的管理协议规范中规定的数据字段长度，对所述应用信息进行分组；

[0172] 组织子模块，用于分别将各组的应用信息组织为相应的通用指令。

[0173] 在本申请的一种优选实施例中，所述系统还可以包括：

[0174] 第一解析模块，用于在接收某一智能卡对所述专有指令的执行结果时，依据该智能卡所符合的管理协议规范将所述执行结果解析为通用结果；

[0175] 第二解析模块，用于将所述通用结果解析为业务数据；

[0176] 业务处理模块，用于依据所述业务数据进行相应的业务处理。

[0177] 对于系统实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0178] 本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0179] 以上对本申请所提供的一种智能卡的多应用管理方法和系统，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

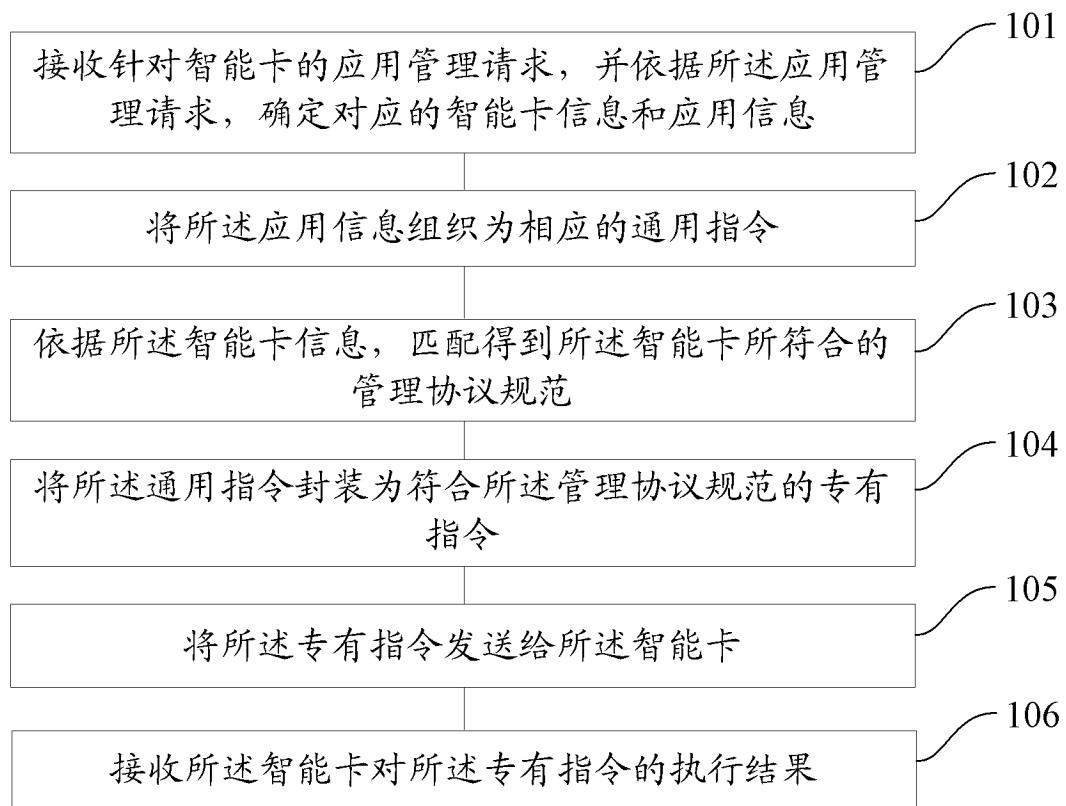


图 1

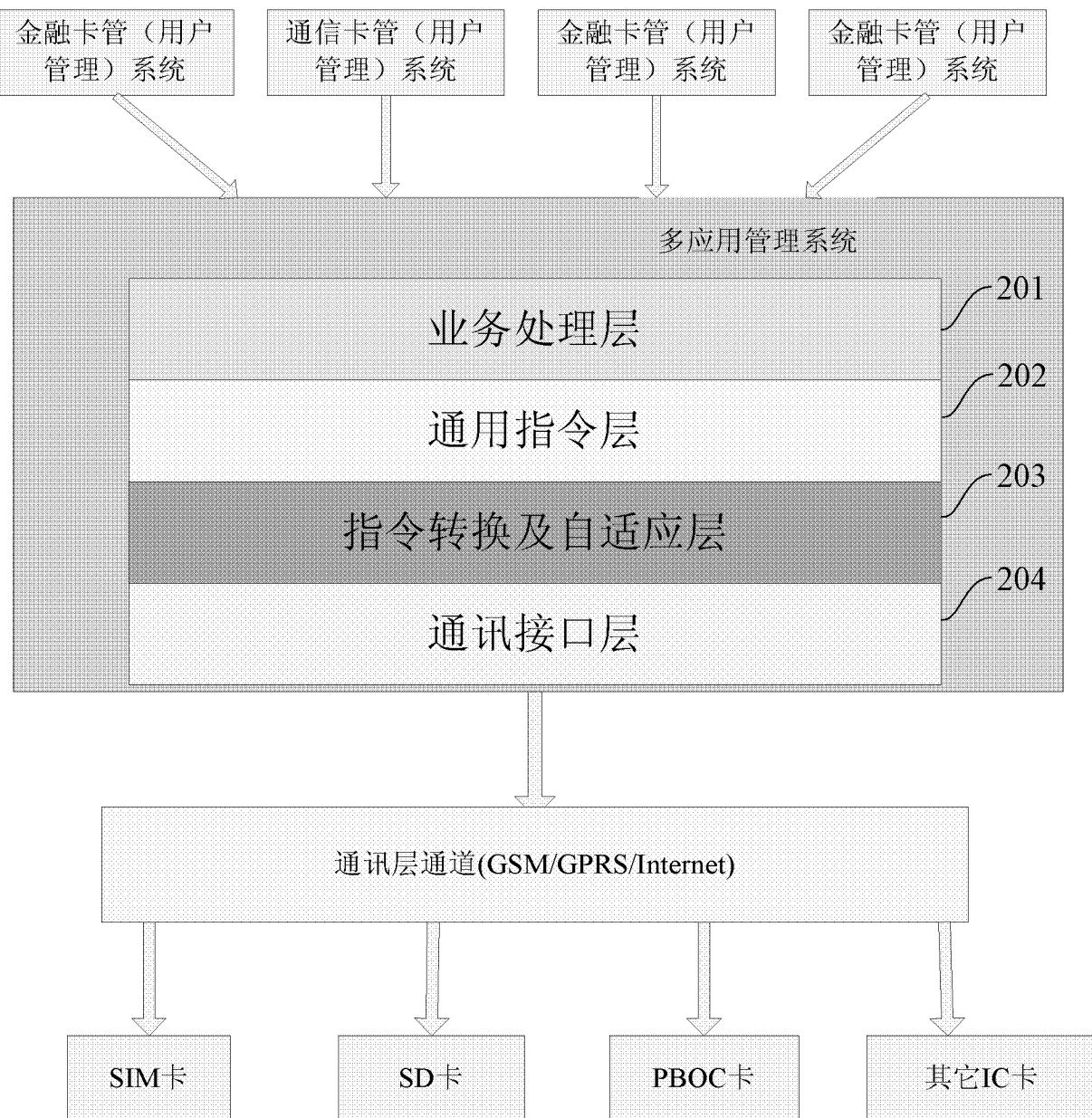


图 2

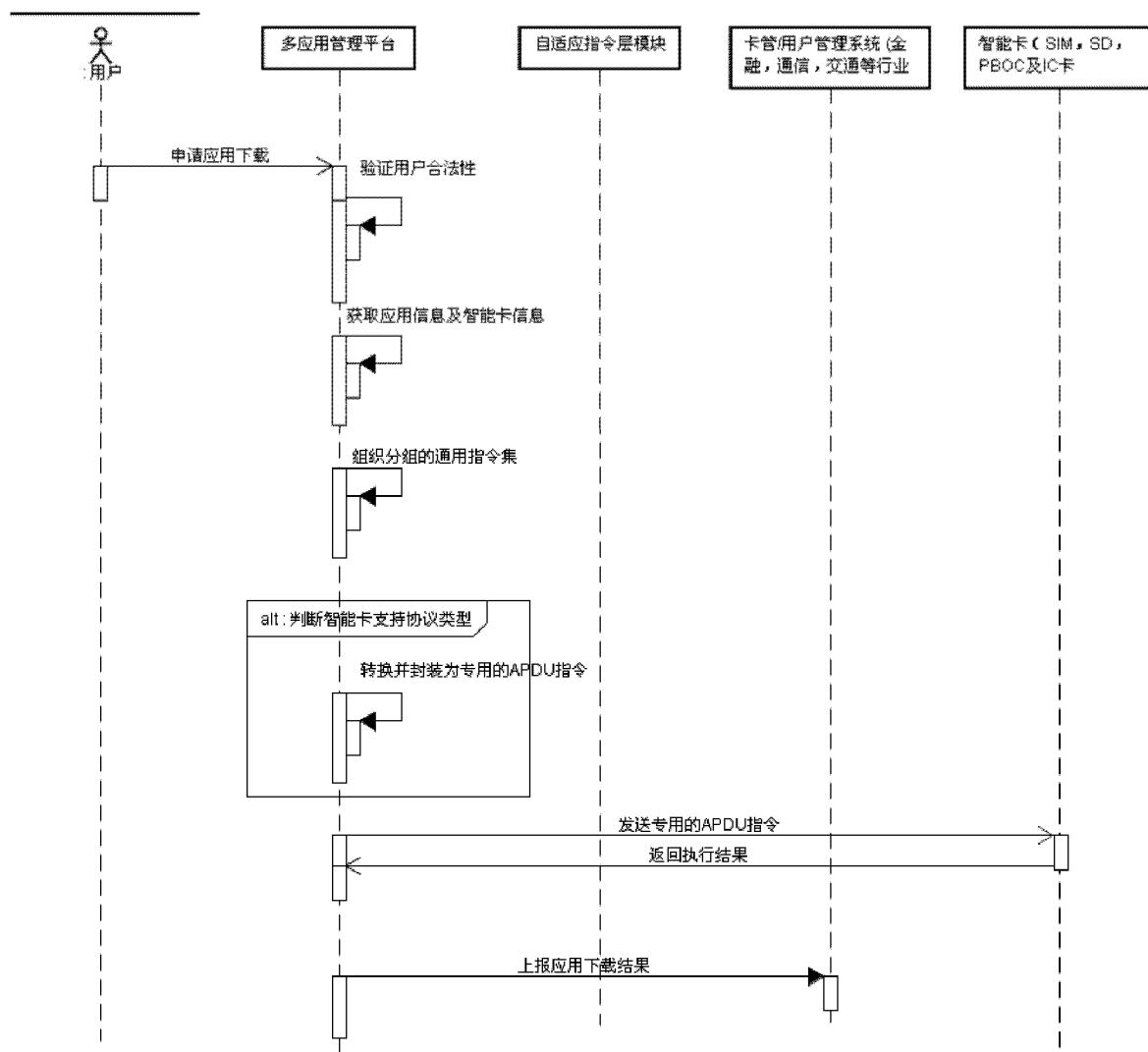


图 3

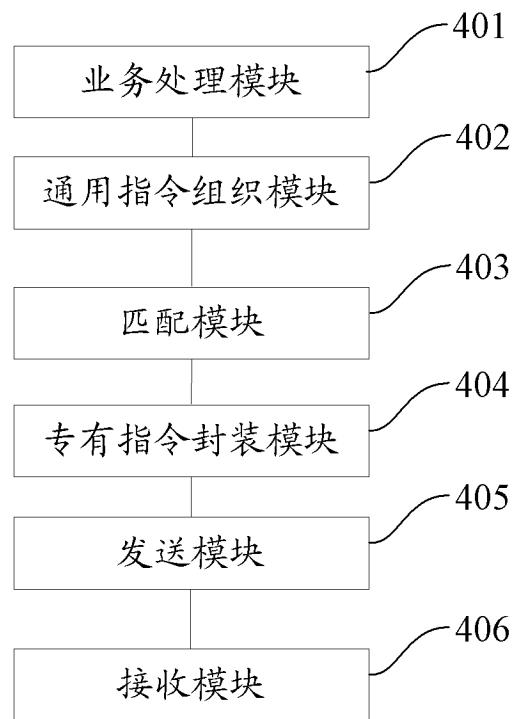


图 4